Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Contents

		Page
I.	Introduction	3
II.	Freedom of expression, States and the private sector in the digital age	4
	A. International legal framework	4
	B. A framework for private sector responsibilities	5
III.	Private sector roles and public/private regulation	6
	A. Impact of private enterprise on freedom of expression	6
	B. Regulation in the digital age	8
IV.	Legal and policy issues	10
	A. Content regulation	10
	B. Surveillance and digital security	15
	C. Transparency	17
	D. Remedies	18
V.	Further thematic development	19
VI.	Conclusions and recommendations	21

I. Introduction

1. The private sector's role in the digital age appears pervasive and ever-growing, a driving force behind the greatest expansion of access to information in history. Vast social media forums for public expression are owned by private companies. Major platforms aggregating and indexing global knowledge, and designing the algorithms that influence what information is seen online, result from private endeavour. The infrastructure for mobile technology, by which billions communicate and reach the Internet, depends upon private investment, maintenance and ownership. The tools for law enforcement and intelligence are often drawn from products of the private surveillance and data-processing industries. Private companies design, manufacture and often maintain the devices or services on which the most important personal data are stored — from financial and health-care information to e-mails, text messages, search histories, photographs and videos.

2. The contemporary exercise of freedom of opinion and expression owes much of its strength to private industry, which wields enormous power over digital space, acting as a gateway for information and an intermediary for expression. In digital environments, important questions about applicable law and the scope of private authority and public regulation cannot be avoided. Should these private actors have the same responsibilities as public authorities? Should their responsibilities derive from human rights law, terms of service, contractual arrangements, or something else? How should relationships among corporate actors and States be structured? When faced with pressures to conduct their businesses in ways that interfere with freedom of expression, what steps should private actors take? Refuse to enter markets or withdraw from them? Advise their customers about such pressures? As the world moves ever more deeply into digital space, with the "Internet of things" on the near horizon, guidance is critical to ensure rights are promoted, protected and enjoyed.

3. The present report has several aims.[1] First, it seeks to identify the categories of private actors that deeply influence the freedom of expression in a digital age. Secondly, it identifies questions concerning both the private sector's protection of freedom of opinion and expression and public authorities' responsibility to ensure the protection of space for expression. Thirdly, it lays out several areas in which normative guidance appears to be most needed. These areas will be addressed and consolidated through thematic reporting, country and company visits, and communications and consultations with Governments, the business sector and civil society. In short, the present report is the first of several the Special Rapporteur will present in order to provide guidance on how private actors should protect and promote freedom of expression in a digital age.

4. Public process of input and consultation contributed to the development of the present report. On 3 December 2015, the Special Rapporteur issued a call for input to the report. As of the date of publication, the Special Rapporteur received 15 submissions from States[2] and 15 submissions from organizations[3], all of which are to be found on the Special

---

[1] The Special Rapporteur would like to thank his legal adviser, Amos Toh, and his students at the University of California, Irvine School of Law, for their assistance with the preparation of this report.

[2] Armenia, El Salvador, Estonia, Greece, Jordan, Kuwait, Mauritius, Mexico, Netherlands, Peru, Republic of Moldova, Romania, Slovakia, Turkey and United States of America.

[3] Article 19; Association for Progressive Communications; Center for Democracy and Technology; Center for Technology and Society; Centre for Communication Governance at National Law University, New Delhi; Danish Institute for Human Rights; Derechos Digitales; European Digital Rights; Freedom Online Coalition Working Group on Privacy and Transparency Online; Global Network Initiative; Institute for Human Rights and Business; International Centre for Not-for-Profit

Rapporteur's website.[4] The Special Rapporteur also benefited greatly from consultations. He held a meeting on 25 and 26 January 2016 with 25 members of civil society at the University of California, Irvine School of Law, and a separate meeting with 20 individuals from the private sector and civil society on 29 February 2016 at the Office of the United Nations High Commissioner for Human Rights in Geneva. Meeting summaries are also be found on the Special Rapporteur's website.

II. Freedom of expression, States and the private sector in the digital age

5. This mapping report rests on a basic question: to what extent should the information and communications technology sector be responsible for the promotion and protection of freedom of opinion and expression? Addressing this question requires beginning with a summary of the international human rights law according to which States are obligated to promote and protect freedom of expression and principles addressing private-sector human rights responsibilities.

A. International legal framework

6. Article 19 of both the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights protects everyone's right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. It has become customary to emphasize that individuals enjoy the same rights online as they do offline. The previous mandate holder highlighted the increasing number and forms of restrictions on the right to information online (see A/HRC/17/27) and demonstrated the impact on freedom of expression of expanded digital surveillance (see A/HRC/23/40). In 2015, the Special Rapporteur emphasized the important role played by encryption and anonymity in protecting and advancing the freedom of expression (see A/HRC/29/32). In joint declarations, the Special Rapporteur and regional counterparts have emphasized issues relating to intermediary liability, access, content restrictions and other key topics on freedom of expression online.

7. Article 19 (3) of the International Covenant on Civil and Political Rights allows for restrictions on the freedom of expression (but not on the freedom of opinion under article 19 (1)). According to article 19 (3), any restriction, to be legitimate, must be provided by law and necessary for the respect of the rights or reputations of others or the protection of national security or of public order, or of public health or morals. Any restriction must be precise enough and publicly accessible in order to limit the authorities' discretion and provide individuals with adequate guidance (see the Human Rights Committee's general comment No. 34 (2011) on article 19: freedoms of opinion and expression). To be necessary, a restriction must be more than merely useful, reasonable or desirable.[5] It is also well established that necessity requires an assessment of proportionality (see A/HRC/29/32). Proportionality requires demonstrating that restrictive measures are the least intrusive instrument among those which might achieve their protective function and proportionate to the interest to be protected (see general comment No. 34). When

---

Law; Internet Society; Korean Progressive Network Jinbonet; Privacy International; Ranking Digital Rights; and New America.

[4] Available from www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx.

[5] European Court of Human Rights, Application No. 6538/74, *The Sunday Times v. The United Kingdom* (26 April 1979), para. 59.

restrictions fail to meet the standard of article 19 (3), individuals enjoy the right to an effective remedy under article 2 (3) of the Covenant.

8. Individuals enjoy the full range of other rights online as well, such as privacy, religious belief, association and peaceful assembly, education, culture and freedom from discrimination. States have both a negative obligation to refrain from violating rights and a positive obligation to ensure enjoyment of those rights. These positive obligations may require public authorities to take steps to protect individuals from the actions of private parties.[6]

B. A framework for private sector responsibilities

9. Human rights law does not as a general matter directly govern the activities or responsibilities of private business. A variety of initiatives provide guidance to enterprises to ensure compliance with fundamental rights. The Human Rights Council endorsed the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (see A/HRC/17/4 and A/HRC/17/31). Reflecting existing human rights law, the Guiding Principles reaffirm that States must ensure that not only State organs but also businesses under their jurisdiction respect human rights.[7]

10. The Guiding Principles provide a framework for the consideration of private business responsibilities in the information and communications technology sector worldwide, independent of State obligations or implementation of those obligations. For instance, the Guiding Principles assert a global responsibility for businesses to avoid causing or contributing to adverse human rights impacts through their own activities, and to address such impacts when they occur and seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.[8]

11. Due diligence, according to the Guiding Principles, enables businesses to identify, prevent, mitigate and account for how they address their adverse human rights impacts.[9] In the digital environment, human rights impacts may arise in internal decisions on how to respond to government requests to restrict content or access customer information, the adoption of terms of service, design and engineering choices that implicate security and privacy, and decisions to provide or terminate services in a particular market.

12. As a matter of transparency, the Guiding Principles state that businesses should be prepared to communicate how they address their human rights impacts externally, particularly when concerns are raised by or on behalf of affected stakeholders.[10] The United Nations High Commissioner for Human Rights has also urged information and communications companies to disclose risks and government demands transparently (see A/HRC/27/37). Meaningful disclosures shed light on, among other things, the volume and context of government requests for content removals and customer data, the processes for handling such requests, and interpretations of relevant laws, policies and regulations.

---

[6] See general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the International Covenant on Civil and Political Rights. Other norms of international law may apply directly to the activities of private actors, such as the criminalization of crimes against humanity, war crimes and acts of genocide under international humanitarian law.

[7] Guiding Principles on Business and Human Rights, chap. I (A) (1).

[8] Ibid., chap. II (A) (11)-(13).

[9] Ibid., chap. II (A) (17).

[10] Ibid., chap. II (B) (21).

Corporate transparency obligations may also include a duty to disclose processes and reporting relating to terms of service enforcement and private requests for content regulation and user data.

13. Finally, the responsibility to respect involves attention to the availability of remedies — from moral remedies to compensation and guarantees of non-repetition — when the private actor has caused or contributed to adverse impacts.[11]

14. The Guiding Principles provide a useful starting point for identifying private information and communications responsibilities, but several other projects have also proposed principles for the sector. The Global Network Initiative's Principles on Freedom of Expression and Privacy draw on the experience and expertise of the investor, civil society and academic communities. The European Commission published the *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*. Relevant civil society initiatives include the Manila Principles of Intermediary Liability, which establish baseline protection for intermediaries in accordance with freedom of expression standards; the African Declaration on Internet Rights and Freedoms, which promotes human rights standards and principles of openness in Internet policy formulation and implementation on the continent; and the Ranking Digital Rights Corporate Accountability Index, which evaluates a set of major private actors in the digital space on the basis of their adherence to freedom of expression and privacy norms. Civil society also acts to check and balance other actors engaged in Internet governance: the Code of Good Practice on Information, Participation and Transparency in Internet Governance, for example, seeks to ensure that relevant processes are meaningfully communicated to the public, accountable to all stakeholders, and emphasize democratic participation.

III. Private sector roles and public/private regulation

A. Impact of private enterprise on freedom of expression

15. The range of private sector roles in organizing, accessing, populating and regulating the Internet is vast and often includes overlapping categories.[12]

1. Enable connection to the Internet

16. While Internet service providers specifically connect their subscribers to the Internet, telecommunication service providers offer a broader range of services, including access to radio, television, telephone and mobile communication. Major multinational corporations offer both categories of service, not only in their State of origin but also globally. Vodafone, for example, is a British provider that owns and operates networks in 27 countries and has partner networks in over 50 additional countries. TeliaSonera, based in Finland and Sweden, serves markets throughout Eurasia, and MTS Russia provides domestic service but also provides telecommunication services in Armenia, Turkmenistan and Uzbekistan. Companies like these often own and maintain significant aspects of the technical infrastructure that transmit Internet and telecommunications traffic, including fibre optic network cables, satellites or wireless links. Internet service providers in local and

[11] Ibid., chap. II (B) (22).

[12] See, for example, "Strategy panel: ICANN's role in the Internet governance ecosystem" (23 February 2014); R. Mackinnon and others, *Fostering Freedom Online: The Role of Internet Intermediaries* (Paris, UNESCO, 2014); and D. A. Hope, *Protecting Human Rights in the Digital Age* (February 2011).

regional markets might operate a limited number of these networks or lease network capacity from large carriers in order to connect their subscribers to the Internet. State ownership is fairly common among service providers: Switzerland, for example, holds 51 per cent of the shares in Swisscom AG,[13] and Uruguay owns Antel, a major telecommunications provider in the country.[14] While telecommunication and Internet service providers are currently the most common providers of Internet access, a growing number of hybrid companies aim to provide Internet access as well as other Internet-related services.[15]

2. Design and maintain hardware and operating systems that facilitate information processing and Internet access

17. Hardware firms design and manufacture the computer devices that connect individuals to the Internet. The range of devices equipped with personal computing functions is, however, ever-expanding and impossible to cap, given the avalanche of connectedness widely described as the "Internet of things", in which digital connection is enabled for all aspects of contemporary existence. Automobiles, refrigerators, televisions and watches are just a few examples of "smart" devices that today incorporate browser, messaging and other Internet-related functions.

18. Further, telecommunication and Internet service providers purchase equipment and other network components that comprise the physical backbone of their networks from infrastructure vendors and equipment manufacturers. These products can range from simple routers and switches to deep packet inspection devices, network filtering and Internet blocking devices, and surveillance monitoring centres. Increasingly these companies also include services, consulting, training and even operation.

3. Allocate web domains

19. Internet addresses (that is, uniform resource locators (URLs)) are allocated and sold by domain name registries and registrars, under the supervision of the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit entity. Currently, the world's largest registrar hosts more than 61 million domain names.

4. Host information

20. Web-hosting services enable users to upload and deliver files and other materials to their readers' or customers' browsers. These companies typically also provide data storage, e-mail and other services associated with the websites their customers have purchased.

5. Facilitate aggregating, sharing and searching for information

21. Search engines supply the vital connection between users who search for information, and those who create, aggregate and publish it. Indeed, search engine algorithms dictate what users see and in what priority, and they may be manipulated to restrict or prioritize content. Information searches, however, are not unique to search engines. Content aggregators, specialized research services, social media platforms and professional networks also enable users to search for content.

---

[13] See www.swisscom.ch/en/about/investors/shares/ownership-structure.html.

[14] See www.antel.com.uy/antel/; http://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/latin-america/uruguayIntro.html.

[15] Google, for example, will provide access to wireless service through its Google Fiber service, in addition to its search, content-hosting and social networking functions, among others. See https://fiber.google.com/about/.

6. Produce and regulate access to one's own content

22. Companies that create or purchase content produced on their platforms often hold the copyright to such content, enabling them to monetize and manage access to it. Some of the most influential copyright holders are media and entertainment companies, including news media, publishing houses, music labels, and film and television studios.

7. Connect users and communities

23. Companies also provide a variety of services that connect users across multiple platforms, including e-mail, web chats, discussion threads, and social and professional networking. The most prominent actors in this area include e-mail providers, social media and other networking platforms, and online bulletin boards. In addition to such platforms, news websites, e-commerce platforms and application stores provide opportunities for the sharing of information and ideas through reviews, comments and discussions. Internet payment systems also integrate a social networking functionality.

8. Sell goods and services and facilitate transactions

24. E-commerce facilitates the sale of goods and services and other commercial transactions among businesses and consumers, businesses and other businesses, or consumers and other consumers. The ways in which companies provide access to, promote, or arrange these transactions, and safeguard the wealth of personal information generated by these transactions, may implicate the freedom of expression and privacy of their customers.

9. Collect, repurpose and sell data

25. The vast majority of enterprises described above collect information from and about their users, which in turn may be used to target advertising, customize existing services, reduce security risks, or shut down accounts of abusive users. Companies may, however, also trade in information collection and analysis, involving such services as designing, customizing or selling surveillance and information analytics technologies, or provide consulting services that facilitate law enforcement, intelligence, cybersecurity and surveillance operations.

B. Regulation in the digital age

26. The regulatory ecosystem on the Internet is extensive and diverse, involving actors at domestic, regional and international levels, in private and public sectors, in academia and civil society. Some aspects of information and communications technology — such as the provision of telecommunication and Internet services — have long attracted State and international regulation as well as public scrutiny. Other areas, such as search, social media, and the sale of surveillance technologies, are also increasingly subject to such scrutiny, commensurate with their growing impact and influence on the exercise of freedom of expression online.

1. Technical standards

27. Technical standards and processes ensure that the infrastructure, networks and applications that comprise Internet and telecommunication networks operate seamlessly. The physical infrastructure on which Internet traffic flows, such as network cables and satellites, are set up and run according to various technical requirements that ensure their smooth functioning. Organizations that develop such requirements include the International Telecommunication Union, which sets standards for the interoperability of

telecommunication networks; the Institute of Electrical and Electronic Engineers, a professional association which develops standards for Wi-Fi transmission; and the Groupe Speciale Mobile Association, a private international association of the mobile industry which develops standards for mobile networks.

28. Another group of organizations establishes and develops technical standards for how Internet data are communicated, stored, arranged and presented. The Internet Engineering Task Force develops and maintains the Transmission Control Protocol/Internet Protocol, which determines how devices connect over the Internet and how data are transmitted between them. The World Wide Web Consortium sets standards concerning the display of, and interaction with, web content, which implicates issues such as language content and access for the disabled. ICANN sets policies for the registration of top-level domain names, whether generic (such as .com, .org, .edu), country code (.cn, .tj, .sg) or community or industry-specific (such as .aero). Its subsidiary, the Internet Assigned Numbers Authority, manages the distribution of Internet Protocol addresses, which assign and identify each device that connects to the Internet with unique numerical labels.

29. While technical standards have profound implications for freedom of expression, the Commission on Science and Technology for Development of the United Nations has observed that standards development often lacks sufficient consideration of human rights concerns.[16] To be sure, interested stakeholders and members of the public are permitted to participate in or observe the work of most of these standard-setting bodies. However, because meaningful participation requires a generally high level of technical expertise, human rights perspectives are not always included in discussions, even though technical and design choices can have a substantial impact on freedom of expression.[17]

2. Internet governance and policymaking

30. International legal instruments do not explicitly address how States and other actors should maintain a free and open Internet, nor may regulation by law always be an appropriate approach. Indeed, Internet governance is not the sole province of specialized bodies or Governments. Most recently, the World Summit on the Information Society emphasized the continuing importance of a governance approach that integrates government, corporate and civil society, academic and technical stakeholders and expertise (see General Assembly resolution 70/125). In the context of global trade, non-discrimination principles established under international agreements administered by the World Trade Organization may require States to restrict or otherwise regulate non-neutral services. The World Intellectual Property Organization has also faced growing demands from member States for advice on legislative frameworks that enable them to implement treaty obligations in digital environments. Regional bodies, such as the African Union, the European Commission and the Organization of American States seek to ensure that global

[16] See Intersessional Panel of the Commission on Science and Technology for Development, "The mapping of international Internet public policy issues" (November 2014).

[17] To be sure, a few organizations have dedicated resources to incorporating human rights perspectives in technical discussions. ICANN, for example, has established a cross community working party on its corporate and social responsibility to respect human rights, which seeks to map and understand the issues and potential solutions relating to corporate and social responsibilities of ICANN from https://community.icann.org/display/gnsononcomstake/CCWP+on+ICANN's+Corporate+and+Social+Responsibility+to+Respect+Human+Rights. A few non-governmental organizations have also made human rights-oriented contributions to technical discussions. See, for example, Neils ten Oever, "Research into human rights protocol considerations", available from https://datatracker.ietf.org/doc/draft-tenoever-hrpc-research/.

Internet policy is formulated and implemented in a manner that takes into account the laws, particularities and concerns of their respective regions.[18]

31. Some organizations that set technical standards have policymaking functions as well. The International Telecommunication Union, for example, develops and coordinates global telecommunications policies. ICANN makes policy judgments about the types of top-level domain names that may be registered and who may claim ownership, in consultation with Governments, the private sector, civil society and other relevant actors.

32. Industry-led initiatives also seek to address Internet governance challenges that are insufficiently addressed by existing legal regulation. The Copyright Alert System, for example, brings together trade associations in the film and recording industries and Internet service providers to develop and implement a unified approach to combating copyright infringement online. The Telecommunications Industry Dialogue brings together telecommunications operators and vendors to address freedom of expression and right to privacy concerns in their sector.

33. While many of these initiatives are privately run, they sometimes collaborate with or receive support from States. For example, the Internet Watch Foundation of the United Kingdom of Great Britain and Northern Ireland, which provides Internet service providers and hosting platforms with a "notice and takedown" service that alerts them to potentially criminal content on their networks, also provides law enforcement agencies with "unique data" in their investigations of such content.

IV. Legal and policy issues

34. The information and communications technology sector's multiple roles raise legal and policy questions that deserve attention and elaboration by international human rights mechanisms.

A. Content regulation

35. Many questions concerning private actors in the digital age focus on content regulation. For instance, how do States facilitate or demand content removal, censorship and unnecessary or disproportionate restrictions on the right to seek, receive and impart Internet content through private platforms and networks? How do private enterprises respond to these demands and other external pressures? When the private sector develops and enforces its own internal policies and standards to protect and promote rights online, how do these have an impact on individual expression and access information?

36. Digital content transmitted on private networks and hosted on private platforms is increasingly subject to State and corporate regulation. The universe of user-generated content is always expanding — blogs, text messages, discussion threads, photographs, videos and social media postings are only a sample of the types of content that users create and share on a daily basis. Companies that manage networks and platforms for this content, known as intermediaries, may "give access to, host, transmit and index content, products

[18] See, for example , European Commission, *ICT Sector Guide* (para. 14 above); and Inter-American Commission on Human Rights, Office of the Special Rapporteur for Freedom of Expression, *Freedom of Expression and the Internet* (2013).

and services originated by third parties" even though they do not create or produce that content.[19]

37. State demands to remove content are often based on such rationales as defamation, blasphemy, election-related regulations, harassment or hate speech, incitement, intellectual property, obscenity and indecency, terrorist recruitment or "glorification", the protection of national security and public safety, child protection and the prevention of gender-based attacks. Problems long connected to freedom of expression but increasingly complicated in the digital age have also attracted State regulation, including the "right to be forgotten" and pluralism and diversity (for example, network neutrality). Intermediaries themselves establish and enforce terms of service designed to address many of these concerns, for legal, commercial and other reasons. Many of these issues raise questions about the appropriate balance between freedom of expression and other human rights (for example, privacy, non-discrimination). While content regulations are often restrictive in nature, they may also require the transmission of Government-mandated or approved messages,[20] or prohibit differential pricing for content and content delivery services.[21]

1. State regulation

38. States regulate digital content through a variety of legal, political and technical means. Trends of concern include the following.

Vague laws

39. Content regulations are commonly reflected in legislation, court orders or directives or by-laws issued by administrative bodies with delegated authority to manage telecommunications and Internet-related issues. For example, China recently amended its cybersecurity law to forbid persons and organizations from using the Internet to "upse[t] social order" or "har[m] the public interest".[22] Similarly, a draft bill under consideration in Nigeria prohibits anyone from publishing statements in "any medium" with "malicious intent to discredit or set the public against" any person, group or government institution.[23] Such language gives broad discretion to authorities to determine what kinds of digital expression would violate their terms. As a result, individuals and businesses are likely to err on the side of caution in order to avoid onerous penalties, filtering content of uncertain legal status and engaging in other modes of censorship and self-censorship.

Excessive intermediary liability

40. States often require the cooperation of intermediaries to enforce regulations on private networks and platforms. Internet and telecommunication service providers, for example, are required to comply with local laws and regulations as a condition of their operating licences, a legitimate requirement which becomes problematic when the local laws or their implementation are themselves inconsistent with human rights law. Companies less constrained by licensing requirements, such as social networking platforms,

[19] MacKinnon and others, *Fostering Freedom Online*, p. 19; K. Perset, *The Economic and Social Role of Internet Intermediaries* (OECD, 2010).

[20] See Vodafone Group Plc, "Response on issues relating to mobile network operations in Egypt" (2011).

[21] India, for example, prohibits service providers from offering or charging discriminatory tariffs for data services on the basis of content (Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016).

[22] China, Cybersecurity Law (2015), art. 9.

[23] Parliament of Nigeria, A bill for an act to prohibit frivolous petitions and other matters connected therewith, sect. 3 (3).

search engines and domain name registrars, nevertheless face the threat that States will disrupt local infrastructure, threaten the safety of local employees, or block local access to their platforms.

41. Private actors may also request intermediaries to restrict or remove content. For instance, intellectual property complaints often arise when a private party alleges that a person has shared or used content in a manner that violates its copyright or has created a domain name that violates its trademark. While fair use and other defences to such complaints may be available, intellectual property frameworks may inhibit cultural and artistic expression (see A/HRC/28/57).

42. The European Court of Justice, in *Google Spain v. Mario Costeja González*, compelled Google under the Data Protection Directive of the European Union to delist search results based on web pages that identified González, even though the original publication of those pages was itself not subject to takedown.[24] The decision has found an active life outside the European context.[25] The scope and implementation of this approach raise questions about the appropriate balance between the rights to privacy and protection of personal data on one hand, and the right to seek, receive and impart information containing such data on the other.

43. Intermediaries are increasingly required to assess the validity of State requests and private complaints against general legal criteria, and remove or delink such content based on such assessments. For example, the Cybercrime Act, 2015 of the United Republic of Tanzania only exempts hyperlink providers from liability for information linked provided that they "immediately remove[ ] or disable[ ] access to the information after receiving an order to do so from the relevant authority".[26] In the context of copyright, the Digital Millennium Copyright Act of the United States of America exempts providers of "online services and network access" from liability for third party content only if they respond "expeditiously to remove, or disable access to the material that is claimed to be infringing or to be the subject of infringing activity" upon notice of such infringement.[27] These notice and takedown frameworks have been criticized for incentivizing questionable claims and for failing to provide adequate protection for the intermediaries that seek to apply fair and human rights-sensitive standards to content regulation.

44. Another major concern is that private intermediaries are typically ill equipped to make determinations of content illegality. The Inter-American Commission on Human Rights has observed that private actors "lack the ability to weigh rights and to interpret the law in accordance with freedom of speech and other human rights standards".[28] This may be due to resource constraints, lack of oversight and accountability, or potential conflicts of interest. In the face of potential liability, companies may be prone to self- or over-censorship.

Extralegal restrictions

45. States also seek to restrict digital content outside the law. Some States have pushed for social media companies and other hosts of user-generated content to monitor and take down content on their own initiative, rather than wait for law-based requests from the Government. Government officials have also attempted to persuade companies to adopt "counter-speech" initiatives through public forums, campaigns and in private discussions.

---

[24] Judgment of the European Court of Justice (Grand Chamber), case C-131/12 (13 May 2014).
[25] Submission of Article 19.
[26] Para. 43 (a).
[27] United States Code, title 17, sect. 512 (c) (1) (C).
[28] Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, pp. 47-48.

Governments are also increasingly flagging content on social media as inappropriate under a platform's terms of service, in order to prompt the company to remove the content or deactivate an account.

Filtering

46. States often block and filter content with the assistance of the private sector. Internet service providers may block access to specific keywords, web pages or entire websites. On platforms that host content, the type of filtering technique depends on the nature of the platform and the content in question. Domain name registrars may refuse to register those that match a government blacklist; social media companies may remove postings or suspend accounts; search engines may take down search results that link to illegal content. The method of restriction required by Governments or employed by companies can raise both necessity and proportionality concerns, depending on the validity of the rationale cited for the removal and the risk of removal of legal or protected expression.

47. Ambiguities in State regulation coupled with onerous intermediary liability obligations could result in excessive filtering. Even if content regulations werevalidly enacted and enforced, users may still experience unnecessary access restrictions. For example, content filtering in one jurisdiction may affect the digital expression of users in other jurisdictions. While companies may configure filters to apply only to a particular jurisdiction or region, there have been instances where they were nevertheless passed on to other networks or areas of the platform. For instance, in 2013 State-mandated filtering carried out by Airtel India led to restrictions on the same content on several networks in Oman belonging to its partner, Omantel.[29]

Network or service shutdowns

48. Service shutdowns and associated restrictions are a particularly pernicious means of enforcing content regulations. Such measures are frequently justified on the basis of national security, the maintenance of public order or the prevention of public unrest. In 2015, the Special Rapporteur, together with representatives of the Organization for Security and Cooperation in Europe, the Organization of American States and the African Commission on Human and Peoples' Rights condemned as unlawful Internet "kill switches".[30] In one year alone, there were reports of shutdowns in Bangladesh, Brazil, Burundi, the Democratic Republic of the Congo, India and Pakistan.[31] The Special Rapporteur confirmed instances of telecommunication service provider and service shutdowns in Tajikistan, during his official visit in March 2016.[32]

Non-neutral networks

49. In addition to refraining from unnecessary and disproportionate restrictions on digital access, States also have a duty to ensure a free and open Internet. Network neutrality is the principle that all Internet data, content and services be treated equally and without improper discrimination. However, Internet service providers may deploy technologies that speed up or otherwise favour access to certain content and services, while slowing down others (a practice also known as "throttling"). The growing number of collaborations between Internet service providers and content-hosting platforms that offer free wireless data to access online content or services provided by the latter (also known as the provision of "zero rated" services) has attracted controversy. While such measures detract from the

[29] Citizen Lab, "Routing gone wild: documenting upstream filtering in Oman via India" (2012).

[30] Joint declaration on freedom of expression and responses to conflict situations (2015).

[31] Submission of Institute for Human Rights and Business at 3.

[32] Preliminary observations by the United Nations Special Rapporteur on the right to freedom of opinion and expression, Mr. David Kaye at the end of his visit to Tajikistan (9 March 2016).

principle of net neutrality, it remains a subject of debate whether they may be permissible in areas genuinely lacking Internet access.

50. State regulation in this area is patchy and uncertain. A few States have recognized the general importance of network neutrality. Romania, for example, has stated that it is "in favour of all initiatives to guarantee that online information can be accessed in a meaningful way by the entire population".[33] Fewer States have provided specific legal protection.[34] In early 2016, the Telecom Regulatory Authority of India issued a regulation prohibiting service providers from offering or charging "discriminatory tariffs for data services being offered or charged to the consumer on the basis of content".[35] Some form of network neutrality has been adopted in law or policy by countries including Brazil, Chile, the Netherlands and the United States.

2. Internal policies and practices

51. Intermediaries' policies and rules may have significant effects on the freedom of expressionWhile terms of service are the primary source of regulation, design and engineering choices may also affect the delivery of content.

Terms of service

52. Terms of service, which individuals typically must accept as a condition to access a platform, often contain restrictions on content that may be shared. These restrictions are formulated under local laws and regulations and reflect similar prohibitions, including those against harassment, hate speech, promotion of criminal activity, gratuitous violence and direct threats.[36] Terms of service are frequently formulated in such a general way that it may be difficult to predict with reasonable certainty what kinds of content may be restricted. The inconsistent enforcement of terms of service has also attracted public scrutiny. Some have argued that the world's most popular platforms do not adequately address the needs and interests of vulnerable groups; for example, there have been accusations of reluctance "to engage directly with technology-related violence against women, until it becomes a public relations issue".[37] At the same time, platforms have been criticized for overzealous censorship of a wide range of legitimate but (perhaps to some audiences) "uncomfortable" expressions.[38] Lack of an appeals process or poor communication by the company about why content was removed or an account deactivated adds to these concerns. Terms of service that require registration linked to an individual's real name or evidence to demonstrate valid use of a pseudonym can also disproportionately inhibit the ability of vulnerable groups or civil society actors in closed societies to use online platforms for expression, association or advocacy.

53. States also increasingly rely on terms of service to remove content they find objectionable. The Special Rapporteur on the promotion and protection of human rights while countering terrorism has observed that several States have established content-removal mechanisms that often seek the removal of content that, while lawful, might be regarded as extremist (see A/HRC/31/65). The Counter Terrorism Internet Referral Unit in the United Kingdom, for example, is dedicated to removing online content of a "violent extremist or terrorist nature", including through methods that "use websites' content-

[33] Submission of the Government of Romania.
[34] Mackinnon and others, *Fostering Freedom Online*, p. 80.
[35] Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016.
[36] See, for example, Facebook terms of service, sect. 3 (7); Twitter terms of service; YouTube Community Guidelines; and Reddit.
[37] See https://ourinternet-files.s3.amazonaws.com/publications/no24_web_2.pdf.
[38] See onlinecensorship.org.

flagging mechanisms to report content as a violation of the site's [terms of service]".[39] Such practices raise the prospect that States may rely on private terms of service to bypass human rights or domestic law norms against content restrictions.

54. The work of private censorship is complicated by the sheer volume of complaints and flagged content that intermediaries identify on a daily basis. Large platforms may also outsource content moderation, creating even more distance between content moderators and internal policymaking decisions, and exacerbating inconsistencies in enforcement. Intermediaries that operate in a diverse range of markets inevitably face "complex value judgments", issues with cultural sensitivity and diversity, and "difficult decisions about conflicts of law".[40]

Design and engineering choices

55. The manner in which intermediaries curate, categorize and rank content affects what information users access and view on their platforms. For example, platforms deploy algorithmic predictions of user preferences and consequently guide the advertisements individuals might see, how their social media feeds are arranged and the order in which search results appear.[41] Other self-regulatory measures, such as "counter speech" initiatives to support anti-terror or anti-harassment messages,[42] also affect the ways in which users might consume and process Internet content concerning sensitive topics. It remains an open question how freedom of expression concerns raised by design and engineering choices should be reconciled with the freedom of private entities to design and customize their platforms as they choose.

B. Surveillance and digital security

56. State surveillance and corporate data collection and retention raise substantial issues of freedom of expression. For instance, how do States conduct surveillance activities with the cooperation of the private sector, and how does such cooperation have an impact on freedom of expression? What are the responsibilities of private actors when they discover that States covertly access Internet and telecommunications data transmitted or stored on their networks or platforms? What are the responsibilities of the private sector to protect security and anonymity online?

57. Digital communications and data transmitted or stored on private networks and platforms are increasingly subject to surveillance and other forms of interference, whether by the State or private actors. Unnecessary and disproportionate surveillance may undermine security online and access to information and ideas (see A/HRC/23/40). Surveillance may create a chilling effect on the online expression of ordinary citizens, who may self-censor for fear of being constantly tracked. Surveillance exerts a disproportionate impact on the freedom of expression of a wide range of vulnerable groups, including racial, religious, ethnic, gender and sexual minorities, members of certain political parties, civil society, human rights defenders, professionals such as journalists, lawyers and trade unionists, victims of violence and abuse, and children (see A/HRC/29/32). State capacity to

[39] National Police Chiefs' Council, Counter Terrorism Internet Referral Unit; submission of the Center for Technology and Democracy.

[40] Emily Taylor, *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*, GCIG Paper No. 24 (2016).

[41] Submission of the Center for Technology and Society; Ranking Digital Rights.

[42] See, for example, Home Affairs Committee, Oral testimony of Anthony House, Google Europe, Middle East and Africa (2 February 2016).

conduct surveillance may depend on the extent to which business enterprises cooperate with or resist such surveillance.

1. Requests for customer data

58. As Internet service providers, social networking platforms, search engines, cloud service providers and other companies transmit or amass enormous quantities of customer data, the volume of government requests for user information based on local laws and regulations has also begun to rise. Several major Internet companies have reported an increase in requests.[43] Many of these requests are issued by law enforcement and intelligence agencies. State oversight of these requests varies, ranging from prior judicial authorization[44] to high-level executive approval[45] to none at all. Licensing agreements and the law may limit the ability of the private sector to resist these requests or compel accountability. Even content-hosting platforms, which lack physical presence in certain jurisdictions where they operate, may face the wholesale blocking of their service and attempts to intimidate employees of corporate subsidiaries. Nevertheless, companies in all areas of the information and communications technology industry are capable of establishing and exercising varying degrees of leverage in their relationships with States to resist or mitigate the harm caused by abusive application of the law. Effective strategies of resistance include: the inclusion of human rights guarantees in licensing agreements and other relevant contracts; restrictive interpretations of government requests; negotiations with government officials about the scope of such requests; judicial challenge of overbroad requests or laws; providing affected individuals, the media or public with relevant information; and suspension of service within, withdrawal from, or decisions not to enter a particular market.

2. Sale of surveillance and censorship equipment

59. The private sector supplies hardware, software and other technologies that enable States to intercept, store or analyse communications and other information. Infrastructure vendors, hardware manufacturers and software developers may design or customize products on behalf of States, or supply dual use equipment and technology that States subsequently tailor for their own needs. Internet and telecommunication service providers may also purchase equipment or software from these companies to install on their network components in order to comply with legally mandated interception protocols in the States where they operate. States may rely on these products and services to target, harass or intimidate members of vulnerable groups.

3. Covert surveillance

60. States may also covertly tap into the technical infrastructure belonging to service providers and content platforms in order to intercept a wide variety of information, including communications, user account information, and telephone and Internet records. States reportedly tamper with computer hardware while en route to customers, infiltrate private networks and platforms with malicious software, hack into specific devices, and exploit other digital security loopholes. When business enterprises have notice of such surveillance, questions concerning their human rights responsibilities may arise, such as providing notice to customers or mitigating such harm through security measures. Companies that sell equipment and services to Governments to implement covert

[43] See recent transparency reports from Google, Facebook, Dropbox, Twitter and Microsoft.
[44] Sweden, Act on Signal Surveillance for Defense Intelligence Activities, sect. 4 (3).
[45] Australia, Telecommunications (Interception and Access) Act 1979, sect. 9 (1).

surveillance techniques may be implicated in human rights violations that flow from their sales.

4. Mutual legal assistance treaties and data localization

61. It is important to note that surveillance is affected by other demands on privately held information. For example, the inability of the mutual legal assistance treaty regime to keep pace with cross-border data demands may drive States to resort to invasive extraterritorial surveillance measures. Laws that require companies to retain customer data or store such data in local data centres may also encourage such surveillance.

5. Encryption and anonymity

62. Since the Special Rapporteur reported on the importance of encryption and anonymity for protecting freedom of opinion and expression, government pressure on corporations to compromise the security of their customers' digital devices, communications and information has grown. A range of private entities, from hardware manufacturers to e-mail services to messaging services, have been taking measures to develop and implement technologies that enhance user security, anonymity and privacy. These measures include end-to-end encryption for digital communications, disk encryption and timely software updates to close security loopholes. In response, States are seeking to compel companies to create or exploit technical loopholes in their products and services on their behalf. In the United States, for example, the Federal Bureau of Investigation applied to a federal court to compel Apple to create software that facilitates access to a suspect's iPhone in a terrorism investigation. The Investigative Powers Bill introduced before the British Parliament on 1 March 2016 would authorize intelligence services to apply for a warrant that requires private entities to "secure interference with any equipment for the purpose of obtaining communications [...] equipment data and any other information".[46]

C. Transparency

63. Transparency can help ensure that subjects of Internet regulation are able to meaningfully predict their legal obligations and challenge them where appropriate. Gaps in compliance with these standards threaten the ability of individuals to understand the limits placed on their freedom of expression online and seek appropriate redress when their rights are violated. Transparency issues arise in both State and private sector contexts, such as public-private partnerships, private sector engagement in trade negotiations and the digital arms race.

64. Despite multiple reform attempts, transparency concerning government requests is still lacking. While there has been some improvement in transparency reporting concerning government requests for user information, there is far less information available about the volume and nature of government requests to restrict or remove content.[47] It is unclear whether such statistics are even retained. State restrictions on private disclosures of relevant information can be a major obstacle to corporate transparency. Several States prohibit disclosures concerning government requests for content removal or access to user data. India, for example, prohibits online intermediaries from disclosing details of government orders to block access to Internet content, as well as any action they take in response to

[46] Investigatory Powers Bill (2015), Cl. 88 (2).

[47] Submissions of Freedom Online Coalition Working Group on Privacy and Transparency Online; and Telecommunications Industry Dialogue.

such orders.[48] The British Investigative Powers Bill would prohibit telecommunication service providers from disclosing, among other things, "the existence and contents" of government orders to retain customers' communications data.[49] In other States, ambiguous laws and regulations make it difficult for corporations to determine what kinds of information they are permitted to disclose. In South Africa, for example, private disclosures of government requests for customers' data are prohibited,[50] but it is unclear whether the same restriction extends to content removal requests.[51]

65. In the context of the private sector, service providers and content-hosting platforms often disclose at least some information about the circumstances under which they remove content or comply with government requests for customer data. There is wide variation, however, in whether and how they convey interpretations or explanations of State regulations and terms of service, and internal processes for implementation and enforcement. There are also gaps in corporate disclosure of statistics concerning the volume, frequency and types of request for content removals and user data, whether because of State-imposed restrictions or internal policy decisions. In any case, companies are more likely to disclose statistics concerning government requests than private requests. There has also been far less research into the extent to which other intermediaries (for example, financial or e-commerce intermediaries) and companies disclose information concerning content removals and requests for customer data.

66. Ongoing debate about the minimum standards for corporate disclosures and relevant best practices reflects uncertainty about the appropriate balance between transparency and competing values, such as individual security and trade secrecy. While there is growing consensus that corporations should disclose information about how restrictions are interpreted and enforced, there is less agreement about how this should be done. Similarly, there is widespread agreement about the importance of quantitative transparency, but it is less clear how such information should be contextualized, presented and made accessible.

D. Remedies

67. Restrictions on freedom of expression online occur on a daily basis and frequently involve corporate conduct, whether compelled by law or pursuant to corporate policy and practice (for example, as reflected in terms of service). Common examples of such restrictions include unlawful or otherwise questionable content removals, service restrictions and account suspensions, and data security breaches.

68. Under article 2 (3) of the International Covenant on Civil and Political Rights, States parties must ensure that persons whose rights under the Covenant have been violated have an effective remedy. The Guiding Principles on Business and Human Rights anticipate that corporations should provide remedial and grievance mechanisms that are legitimate, accessible, predictable, equitable, rights-compatible, transparent, based on dialogue and engagement, and a source of continuous learning.[52] There is limited guidance, however, as to how these elements should be operationalized or assessed in the context of information and communications technology. For example, improper removal of web links from search

[48] India, Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009, rule 16.

[49] Investigatory Powers Bill, Cl. 84 (2).

[50] South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, sect. 42 (1).

[51] South Africa, National Key Points Act 102 of 1980, sect. 10 (c).

[52] Guiding principles, chap. III (A) (31).

results might require the search engine to reinstate such links. It is, however, unclear how complaint or appeals mechanisms should be designed and implemented to ensure that such removals are effectively flagged, evaluated and remedied. A search engine's highly dispersed customer base further complicates design issues. It is also unclear whether companies should provide additional remedies, like financial compensation for lost revenue during the period of removal, or guarantees of non-repetition.

69. To enforce terms of service, companies may not always have sufficient processes to appeal content removal or account deactivation decisions where a user believes the action was in error or the result of abusive flagging campaigns. Further research that examines best practices in how companies communicate terms of service enforcement decisions and how they implement appeals mechanisms may be useful.

70. The scope of the corporation's responsibility to remediate is also contested. Who bears the burden of remediating improper removals or data requests when companies interpret or enforce relevant State laws too strictly? When a company's products or services are used to perpetrate human rights abuses, what degree of causation triggers the duty to provide a remedy? When companies face allegations of wrongdoing, is there a duty to conduct internal investigations, and must these investigations meet certain standards? Where a restriction implicates individuals across borders, what jurisdiction is appropriate for the consideration of remedies? These questions reflect the uncertainty that human rights victims face in situations where corporate and State conduct are intertwined.

71. The appropriate role of the State in supplementing or regulating corporate remedial mechanisms also requires closer analysis. Civil proceedings and other judicial redress are often available to consumers adversely affected by corporate action, but these are often cumbersome and expensive. Meaningful alternatives may include complaint and grievance mechanisms established and run by consumer protection bodies and industry regulators. Several States also mandate internal remedial or grievance mechanisms: India, for example, requires corporations that possess, deal with or handle sensitive personal data to designate grievance officers to address "any discrepancies and grievances [...] with respect to processing of information".[53]

V. Further thematic development

72. Given the range of private information and communications technology activity that frames and impacts the exercise of the freedom of opinion and expression online, the Special Rapporteur will focus on State obligations and business responsibilities in specific areas of concern. The legal and policy issues raised above will guide thematic reporting, communications with Governments, country and company visits, regional and expert consultations, and other work.

73. Among the Special Rapporteur's priorities for thematic study and guidance are the following:

Restrictions on the provision of telecommunications and Internet services

74. Governments increasingly require private entities providing telecommunications and Internet service to comply with censorship demands. In addition to network filtering practices, States compel or pressure companies to shut down networks or block entire services. This trend requires further documentation and scrutiny. Future work will examine

[53] India, Information Technology Act, 2008, sect. 43 A; Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, rule 5 (9).

laws, policies and extralegal measures that enable Governments to undertake such restrictions, and the costs and consequences of such restrictions. The Special Rapporteur will also examine the responsibilities of companies to respond to such measures in a way that respects rights, mitigates harm and provides avenues for redress where abuses occur.

Content restrictions under terms of service and community standards

75. Private actors face substantial pressures from Governments and individuals to restrict expression deemed to constitute extremism or hatred, hostility or harassment. Private actors may also themselves aim to foster what they perceive to be civil discourse on their platforms, regulate access through real-name requirements and other registration policies, or feature or prioritize certain content for business reasons. Future work will evaluate the potential of State abuse of private initiatives, the impact of private measures on freedom of expression, and the relevant human rights obligations and responsibilities. This reporting will not only focus on the roles of social media and search engines, but also lesser known actors such as e-commerce and financial intermediaries.

Liability for content hosting

76. Intermediaries are increasingly held responsible for third party content that they host, whether through intermediary liability regimes or censorship requirements. Commonly cited rationales for such restrictions include cybersecurity, copyright, defamation and data protection. Further study will focus on the legitimate scope of such rationales, the necessity of accompanying restrictions, and the lack of procedural safeguards under existing frameworks for removing third party content. Future work will also examine sources and modes of intermediary liability in particular contexts and regions and seek to draw out the main principles and practices applicable in order to ensure the ability of intermediaries to promote and protect freedom of expression.

Censorship and surveillance industry

77. Private companies play a major role in the development, production and transfer of software and hardware that Governments may deploy for law enforcement, intelligence and public security purposes. While such tools may have legitimate purposes, they are often deployed by Governments for purposes of censorship and disproportionate surveillance. Future work will explore such issues through the human rights framework and encourage due diligence in identifying the uses of such technologies for purposes that undermine freedom of expression.

Efforts to undermine digital security

78. Companies that transmit, store or generate communications and other forms of user data — particularly telecommunication and Internet service providers, and content-hosting platforms — face mounting demands from law enforcement and security services for access to their customers' information. Future work will seek to identify approaches that could maximize the scope for freedom of expression while nonetheless addressing legitimate governmental interests in national security and public order.

Internet access

79. The billions of individuals who are connected online enjoy access to information and ideas that is denied billions more who lack the infrastructure or political, security, legal or social environment necessary for connectivity. As the private sector increasingly seeks to empower the next billions with access, it will be critical to ensure that such access is free, open and secure. Future work will explore issues around access and private sector

engagement and investment in ensuring affordability and accessibility, particularly considering marginalized groups.

Internet governance

80. The outcome of the World Summit on the Information Society demonstrated the continuing broad support for multi-stakeholder governance of the Internet. The existing model nonetheless faces increasing pressure in the form of specific national policies (such as data localization) and strategies such as "cybersovereignty". Moreover, there is a persistent need to maintain or increase human rights participation at all levels of governance, including the setting of technical standards, and to ensure that Internet governance frameworks and reform efforts are sensitive to the needs of women, sexual minorities and other vulnerable communities.

81. Throughout this future work, the Special Rapporteur will pay particular attention to legal developments (legislative, regulatory, and judicial) at national and regional levels. In this context, he alerts all stakeholders to his interest in gathering such materials for future communications and reporting and encourages interested parties to collect and provide such material throughout the course of this work.

VI. Conclusions and recommendations

82. The information and communication technology sector is always in rapid development, continually upgrading technology, digitizing everyday life. As a result, addressing legal and policy issues with an eye to current normative gaps involves some risk of failing to address trends that are only now emerging or have yet to emerge. This is a natural feature of the digital age, but even with rapid change in technology, the digital environment will continue to be animated by persistent threats to freedom of opinion and expression. These threats include government dominance of, or attempts to dominate, sources of information, using tools of censorship against online services and infrastructure; the struggle of businesses to promote their products and services in environments that are hostile to freedom of expression; the failures of many business enterprises to ensure the promotion and protection of rights in their pursuit of commercial interests; and the often contradictory demands of individuals that business entities provide them not only with security but also convenience, connectivity and community. As the project of exploring information and communication technology responsibilities moves forward, the Special Rapporteur will be looking to experts in the field —in Government, the private sector, civil society, the technical community, academia — to help him conduct analysis and reporting that respond both to the current issues at the intersection of technology and freedom of expression and to long-term features of the digital age.

83. The Special Rapporteur strongly encourages all stakeholders — whether State actors, private sector enterprises or civil society organizations and individuals — to take an active part in the development of the forthcoming projects. He particularly encourages stakeholders from less developed countries and vulnerable communities to share perspectives on the impact that the information and communication technology sector may have on the enjoyment of rights and the role that States may play in either interfering with or advancing those rights.

84. Even though this project is at its early stages, it is nonetheless critical that States and private actors take steps to ensure respect for the freedom of opinion and expression. These steps should include, at a minimum, the following, with further analysis to follow throughout the Special Rapporteur's mandate.

States

85. States bear a primary responsibility to protect and respect the right to exercise freedom of opinion and expression. In the information and communication technology context, this means that States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means. Any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19 (3) of the International Covenant on Civil and Political Rights. Particularly in the context of regulating the private sector, State laws and policies must be transparently adopted and implemented.

86. Governments must also adopt and implement laws and policies that protect private development and the provision of technical measures, products and services that advance freedom of expression. They must ensure legislative, policymaking and other relevant norm-setting processes concerning rights and restrictions on the Internet in order to provide the private sector, civil society, the technical community and academia meaningful opportunities for input and participation.

Private sector

87. States place undeniable pressures on the private information and communication technology sector that often lead to serious restrictions on the freedom of expression. The private sector, however, also plays independent roles that may either advance or restrict rights, a point the Human Rights Council well understood by adopting the Guiding Principles on Business and Human Rights in 2011 as general guidance in that field. Private entities should be evaluated on the steps they take both to promote and undermine freedom of expression, even in hostile environments unfriendly to human rights.

88. Among the most important steps that private actors should take is the development and implementation of transparent human rights assessment procedures. They should develop and implement policies that take into account their potential impact on human rights. Such assessments should critically review the wide range of private sector activities in which they are engaged, such as the formulation and enforcement of terms of service and community standards on users' freedom of expression, including the outsourcing of such enforcement; the impact of products, services and other commercial initiatives on users' freedom of expression as they are being developed, including design and engineering choices, and plans for differential pricing of or access to Internet content and services; and the human rights impact of doing business with potential government customers, such as the operation of telecommunication infrastructure or the transfer of content-regulation or surveillance technologies.

89. It is also critical that private entities ensure the greatest possible transparency in their policies, standards and actions that implicate the freedom of expression and other fundamental rights. Human rights assessments should be subject to transparent review, in terms of their methodologies, their interpretation of legal obligations and the weight that such assessments have on business decisions. Transparency is important across the board, including in the context of content regulation, and should include the reporting of government requests for takedowns.

90. Beyond adoption of policies, private entities should also integrate commitments to freedom of expression into internal policymaking, product engineering, business

development, staff training and other relevant internal processes. The Special Rapporteur will aim to explore policies and the full range of implementation steps in a number of ways, including through company visits.

International organizations and multi-stakeholder processes

91. As the present report has shown, many international organizations play a role in information and communication technology governance processes. It is critical that such organizations provide meaningful public access to policies, standards, reports and other information concerning Internet governance created or generated by the organization and/or its membership, including through facilitating access to free online resources and public education initiatives. More generally, the multi-stakeholder process for Internet governance has been an important driver for policies supportive of freedom of expression. With that in mind, international organizations should ensure meaningful civil society participation in policymaking and other standard-setting processes, including through increasing the presence of technical experts sensitive to human rights concerns.